

# **Exhibit 17**

**SW-SEC00386134**

## INFORMATION SECURITY -

Incident review Sept 2018

## Incident Summary January 2018-Sept 2018



50 incidents from Jan 1 to Sep 10 2018  
compared to 42 incidents for 2017

1 Advisory

35 Minimal – Level 0

33 Low – Level 1

1 Moderate – Level 2

## INCIDENT CLASSIFICATION



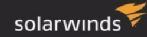
IMPACT/ RISK LEVEL	LEVEL	DESCRIPTION (includes 2 or more)	ILLUSTRATIVE EXAMPLES	IRT REQUIRED
HIGH	3	<ul style="list-style-type: none"> <li>Confirmed information breach / disclosure of sensitive (personal / proprietary) data</li> <li>Impacts a significant segment of SWM customers</li> <li>Disrupts customer facing mission critical IT service(s) for &gt; 1 business days</li> <li>Likely facing severe adverse effect on SWM reputation, revenue, customer(s), partner(s) or the public</li> </ul>	<ul style="list-style-type: none"> <li>Does not include vulnerability or cyber attack in which no data was exfiltrated</li> <li>Significant segment ≥ 50,000 customers / users</li> <li>Most critical disruptions include .coms products, ISP/data center(s) outages and/or large scale B2B, government, academic</li> <li>Involves BU's ability to make quarterly revenue target and / or necessitates CxO press coverage</li> </ul>	YES
MODERATE	2	<ul style="list-style-type: none"> <li>Successful security breach, exposed (to public) security vulnerability, data compromise, or accidental disclosure</li> <li>Meaningful segment of customers / users</li> <li>Disrupts customer facing IT service(s) for &gt; 1 business day</li> <li>Likely adverse effect on SWM reputation, revenue, customer(s), partner(s) or the public</li> </ul>	<ul style="list-style-type: none"> <li>Includes potential and successful breaches</li> <li>Meaningful segment</li> <li>Potential: &gt; 20K customers / users OR Successful: &lt; 50K customers / users</li> <li>Customer facing IT service(s) for &gt; 1 business day (help, support portals, e-comm, demos)</li> <li>Significantly disrupts normal activity for multiple functions (engineering, support, marketing) and/or impacts sales multiple business days</li> </ul>	YES
LOW	1	<ul style="list-style-type: none"> <li>Successful security breach, exposed (to public) security vulnerability, data compromise, or accidental disclosure</li> <li>Modest segment of customers / users</li> <li>Disrupts customer facing service(s) for &lt; 1 business day</li> <li>Likely, but limited adverse effect on SWM reputation</li> </ul>	<ul style="list-style-type: none"> <li>Includes potential and successful breaches</li> <li>Modest segment</li> <li>Potential: &gt; 200K customers / users OR Successful: &lt; 10K customers / users</li> <li>Service disruption for &gt; 4 hrs but less than 1 business day (help, support portals, e-comm, demos)</li> <li>Involves support, marketing, and/or impacts sales for multiple business days</li> </ul>	YES
MINIMAL	0	<ul style="list-style-type: none"> <li>Involves a compromise to public data and/or occurrences of very minor</li> <li>Undetermined security activities or events for which there is no practical follow up</li> </ul>	<ul style="list-style-type: none"> <li>Includes remediation as part of operations and maintenance including scanning, AV reports, network packet capture events, SIEM logging, network firewall reports</li> <li>Isolated system, product, customer issues</li> </ul>	NO

Confidential

© 2018 SolarWinds MSP UK Ltd. All rights reserved.

# Redacted

For the 50 Incidents from Jan1 to Sept 10 2018



**36% of incidents were product related vulnerabilities**

- YTD: 18 - 2017: 14; 28% increase in the number of reported product security incidents.
- Included in this set are vulnerability reports from external security researchers. A number of these are from reputable testing companies engaged by our customers to perform testing.
- The majority of incidents required code changes. Some required hot fixes while others fixes were incorporated into normal build cycles.

**22% of incidents were internal user errors that resulted in potential or actual data exposure.**

- YTD: 11 - 2017: 10
- Data Migration
- Database table merging
- Unintentional user error in product administration
- These incidents could be mitigated by implementing additional controls and verification checks where customer data is in scope.

Confidential

© 2018 SolarWinds MSP UK Ltd. All rights reserved.

## For the 50 Incidents from Jan1 to Sept 10 2018

**14% of incidents were vulnerabilities discovered by generic attacks taken against our web properties.**

- YTD: 7 - 2017: 8
- Bug bounty community is responsible for the majority of these attacks. The researcher is looking for a reward and simply scanning the web for those who will pay a bounty.
- Website vulnerabilities should be resolved but the majority are of low value and criticality
- These can be mitigated by placing an additional layer of protection such as a web application firewall in front of these websites and/or proactively scanning for a baseline of compliance and rescanning as changes occur.

**10% of incidents were the result of Exploitation of a known vulnerabilities in a 3<sup>rd</sup> party component**

- YTD: 5 - 2017: 1; 500% increase in number of reported exploitation of known vulnerabilities.
- Incidents were result of utilizing an unpatched operating system or 3<sup>rd</sup> party component. Establishing secure baselines and applying consistent security updates will help address vulnerabilities being found in this area.

**10% of incidents were from the result of tests initiated by customers.**

- YTD :5 - 2017: 2
- We have seen an increase in internal PEN testing of our products especially by the larger customers.

**6% of all incidents were non-product related issues.**

- Stolen equipment.

**2% of incidents were advisory incidents for tracking**

Confidential

© 2018 SolarWinds MSP UK Ltd. All rights reserved.

For the 50 Incidents from Jan1 to Sept 10 2018

**9 had/have the potential to cause serious damage– 8 out of 9 were discovered and reported internally.**

- RMM Improper or Inappropriate Usage - Elevated RMM access credentials exposed in publicly available Google Doc and if exploited would allow access to all data in RMM
- nCentral Crypto-mining incident discovered internally affected 66 nCentral servers
- Internally reported core communications incident
- Potential compromise of production data in MySQL – MSP Backup – Test server with production data and on the open internet with no security and default password. SQL server compromised (Twice in a week) – No sign of compromise but action taken was forced pw change for all customers. 273,059 users.
- Mail Assure Migration: 2018-018 – 211 Domains out of 2618 had inappropriate data after migration from MaxMail
- BitDefender vulnerability – Force migration to new version of 1.5 million end users in 2.5 months (July-Sep)
- 285 customer Credentials shared with 2 distributors - MSP
- Privileged escalation vulnerability discovered by researcher for myAppOptics.com
- Crypto-mining incidents against Pingdom datacenter provider. KVM switch installed on the server allowed 3<sup>rd</sup> party access and root access to our machine. (Adjust/review our datacenter policies)

Confidential

© 2018 SolarWinds MSP UK Ltd. All rights reserved.

## Highlights

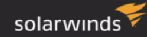


- Internal reporting and fix coordination is critical to reducing the risk of exposure. The more practiced teams proactively engage and embrace the process, but work is still needed for full company adoption.
- Avoidable user errors with data account for a high percentage of the serious incidents.
- No current signs of being a focus of targeted threats. Currently a target of opportunity. This can change at anytime.
- Increase in activity by external parties is not specifically directed towards us but is a trend that will continue.
  - Security researchers are examining our products as part of PEN testing for clients. Core products are most effected.
  - Bug bounty community is active and producing a host of incidents that take time and resources to manage. Being proactive at website scanning can eliminate many of these.
  - Broad based phishing attempts and basic whale hunting attacks have been detected and will continue
  - Broad based server scanning and compromise of weak credentials and known vulnerabilities have been the root cause of incidents
  - Targeted phishing attempts against a set of solarwinds.com email addresses were detected but have been limited
- All incidents have been managed with limited effect on our brand. The incident response process is running well.
- We have managed the process well but we are still at risk. A number of the incidents could have had more serious repercussions. The n-Central crypto-mining issue was the issue that had the most potential impact.

Confidential

© 2018 SolarWinds MSP UK Ltd. All rights reserved.

## Actions to lessen our risk



- **Eliminate incidents**
  - Improve adherence to policy or new policy creation where necessary. User errors account for many of our high risk incidents.
  - Improve security quality on our websites and within our code. The majority of the product incidents that were reported could have been found earlier in the development cycle. Implement the defined SDLC program across the company
- **Discover incidents earlier in the lifecycle**
  - Record, manage, track and appropriately prioritize internally reported security issues (In Process)
  - Extend monitoring to production environments of cloud and MSP
  - Increase active monitoring of O365, Azure AD, Netskope, Akamai, and Palo Alto.
  - Implement SOC services with real time monitoring. (Utilize Threat Monitor)
- **Contain the spread and overall damage incidents can cause**
  - Discover and manage access control for existing users and administrators
  - Implement overall identity management program for privileged users and all users. Use AD as primary source of truth.
  - Validate our network topology and containment strategy

Confidential

© 2018 SolarWinds MSP UK Ltd. All rights reserved.

THANK YOU

Sept 2018

## Security Program Status



- Vulnerability and Patch management – Very Strong program focused on Solarwinds infrastructure including internal servers, Web Properties, Biz Apps.
- Endpoint Security and monitoring of compromise
- Network Segmentation – Network is segmented into Production(TUL), DEV and LAB.
- Next Gen Firewall Deployment and management – Palo Alto FW's are at every site.
- Incident Management/Monitoring via LEM incidents and reports
  - Admin Account Modifications
  - User permission changes
  - System changes, Patches applied
- WAF for Web Properties in progress
- Security Policies
- DLP implementation and monitoring of reports
- Active monitoring and true SOC services
- Identity Management – Role and Privilege management
- Integration of Threat Intelligence

Strong Program  
Needs Improvement  
Limited or non existent

Confidential

© 2018 SolarWinds MSP UK Ltd. All rights reserved.